

UNITED STATES DISTRICT COURT
for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

)
)
)
)
)

Case No. 21-885M(NJ)

Information associated with annefrea22@gmail.com that is
stored at premises owned, maintained, controlled, or operated
by Google LLC, more fully described in Attachment A

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure
of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before June 28, 2021 (not to exceed 14 days)

in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to Nancy Joseph.

(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)

for _____ days (not to exceed 30) until, the facts justifying the later specific date of _____.

Date and time issued: June 14, 2021 @ 10:31 a.m.



Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with annefrea22@gmail.com, as well as all Google, LLC accounts linked to these accounts by cookie values, creation IP addresses, recovery email, SMS recovery, Android device, telephone numbers, and other similar identifiers, that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) January 25, 2021, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account January 1, 2018 through December 31, 2019, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. Stored web history, cloud-based file storage, social networking profile and friends (connections) list;
- d. Text or voice messages, call logs and associated metadata;
- e. The types of service utilized;

- f. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- g. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.
- h. All records relating to user attribution showing who used or owned the device associated with this account including images, documents, logs, communication records;
- i. Evidence indicating how and when the email account was accessed or used, to determine the chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- j. Evidence indicating the geographic location of email access points at times relevant to the investigation;
- k. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- l. All information that constitutes evidence of violations of 18 U.S.C. § 1347 (health care fraud), 18 U.S.C. § 1035 (false statements relating to health care matters); or contraband or other items illegally possessed; or property designed for use, intended for use, or used in committing violations of 18 U.S.C. § 1347 (health care fraud), 18 U.S.C. § 1035 (false statements relating to health care matters)

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1347 and 18 U.S.C. § 1035, those violations involving **Dr. Anne Frea** and occurring after January 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Records of communications related to: (1) the relationship between Dr. Frea and any Medicare provider, DME supplier, physician staffing company or marketing company dealing with Medicare reimbursable services or items, (2) Dr. Frea's work for, or with, any Medicare provider, DME supplier, physician staffing company or marketing company; (3) the prescription or order of Medicare reimbursable services or items for patients; (4) investigations by Medicare or insurance providers regarding prescribed or ordered health care services or items.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT
for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with annefrea22@gmail.com that is
stored at premises owned, maintained, controlled, or operated
by Google LLC, more fully described in Attachment A

)
Case No.
21-885M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

see Attachment A

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 1347
18 U.S.C. § 1035
31 U.S.C. § 3729

Offense Description
Healthcare Fraud
False Statements Relating to Health Care Matters
False Claims Act

The application is based on these facts:

see attached Affidavit.

- Continued on the attached sheet.
 Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under
18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

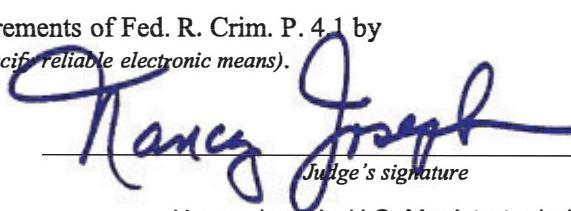

Applicant's signature

Jill Dring, FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone _____ (specify reliable electronic means).

Date: June 14, 2021


Judge's signature

Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jill Dring, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, LLC, an email provider headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since March of 2013. As a Special Agent, I investigate civil and criminal matters related to health care fraud involving violations of the Health Care Fraud Statute, False Claims Act, Anti-Kickback Statute and Stark Law. Prior to investigating health care fraud matters, I investigated criminal and national security related computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of SPAM, malicious software, the theft of identification information, and other computer-based fraud. I have received training in computer technology, computer-based fraud and health care fraud.

3. The facts in this affidavit are known to me through my personal knowledge, training, experience, and through information provided to me by other law enforcement officers in the course of their official duties, whom I consider to be truthful and reliable. This affidavit also relies on Medicare data, which based on my training and experience, I believe to be accurate and reliable.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Relating to Health Care Matters) and 31 U.S.C. § 3729 (False Claims Act) have been committed by Dr. Anne Frea. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated.

PROBABLE CAUSE

I. *Medicare Background*

7. The Medicare Program ("Medicare") is a federally-funded health care program providing benefits to persons who are sixty-five years of age or older, or disabled. Medicare is administered by the Centers for Medicare and Medicaid Services ("CMS"), a federal agency

within the Department of Health and Human Services ("HHS"). Individuals who receive Medicare benefits are referred to as Medicare "beneficiaries."

8. Medicare is a "health care benefit program," as defined by 18 U.S.C. § 24(b).

9. Medicare has four parts: hospital insurance (Part A), medical insurance (Part B), Medicare Advantage (Part C), and prescription drug benefits (Part D). Medicare Part B helps pay the cost of physician services, medical equipment and supplies, and other health services and supplies not paid by Part A.

10. Specifically, Medicare Part B covers medically necessary physician office services, including the ordering of Durable Medical Equipment ("DME"), Prosthetics, Orthotics, and Supplies, such as arm, leg, back, and neck braces ("braces").

11. Suppliers of braces are entities or individuals that are required to enroll with Medicare to become an authorized Medicare provider. Suppliers must complete a Medicare Enrollment Application for Brace Suppliers (CMS Form 855S). That application verifies data by requiring an on-site visit to determine if the supplier meets all of the Medicare Supplier Standards. CMS issues a Medicare supplier number to approved suppliers and maintains a national brace supplier file. If a physician prescribes braces for a Medicare beneficiary, a Medicare-approved and participating supplier must provide it.

12. Section 1847(a)(2) of the Social Security Act defines Off-The-Shelf ("OTS") orthotics as those orthotics described in section 1861(s)(9) of the Act for which payment would otherwise be made under section 1843(h) of the Act, which require minimal self-adjustment for appropriate use and do not require expertise in trimming, bending, molding, assembling, or customizing to fit to the individual. See 42 U.S.C. § 1395w-3. Orthotics that are currently paid

under section 1834(h) of the Act and are described in section 1861(s)(9) of the Act are leg, arm, back, and neck braces. *Id.* § 1395m.

13. The Medicare Benefit Policy Manual (Publication 100-2), Chapter 15, Section 130 provides the Medicare definition of "braces." Braces are defined in this section as "rigid or semi-rigid devices which are used for the purpose of supporting a weak or deformed body member or restricting or eliminating motion in a diseased or injured part of the body."

14. By becoming a participating provider in Medicare, enrolled providers agree to abide by the policies and procedures, rules, and regulations governing reimbursement. To receive Medicare funds, enrolled providers, together with their authorized agents, employees, and contractors, are required to abide by all provisions of the Social Security Act, the regulations promulgated under the Act, and applicable policies, procedures, rules, and regulations issued by CMS and its authorized agents and contractors. Health care providers are given and provided with online access to Medicare manuals and services bulletins describing proper billing procedures and billing rules and regulations.

15. Health care providers may only submit claims to Medicare for reasonable and medically necessary services that they rendered. Medicare does not pay claims procured through kickbacks and bribes or based on falsified medical records.

16. For certain DME products, such as OTS knee braces billed under codes L1833 and L1851, orders are deemed not reasonable and necessary unless the ordering/referring physician documents knee instability using an objective description of joint laxity determined through an examination.

17. Medicare uses the term "ordering/referring" provider to identify the physician who ordered, referred, or certified an item or service reported in that claim. A provider "orders"

non-physician items or services for the beneficiary, such as braces, clinical laboratory services, or imaging services.

18. Medicare requires ordering/referring physicians to document medical necessity and other coverage for braces. Medicare regulations require health care providers enrolled with Medicare to maintain complete and accurate patient medical records reflecting the medical assessment and diagnoses of their patients, as well as records documenting actual treatment of the patients to whom services were provided and for whom claims for payment were submitted by the physician. Medicare requires complete and accurate patient medical records so that Medicare may verify that the services were provided as described on the claim form. These records are required to be sufficient to permit Medicare, through its contractors, to review the appropriateness of Medicare payments made to the health care provider. Brace suppliers are required to maintain copies of these records for six years and three months and to make them available upon request.

19. To receive reimbursement from Medicare for non-physician items such as OTS orthotics, a brace supplier is required to submit a claim, either electronically or in writing, through Form CMS-1500 or UB-92. Claim forms require important information, including: (a) beneficiary's name and identification number; (b) the name and identification number of the referring/ordering provider who ordered the OTS orthotics; (c) the health care benefit item that was provided or supplied to the beneficiary; (d) the billing codes for the specified item; and (e) the date upon which the item was provided or supplied to the beneficiary.

II. *National Investigation by the FBI and the Department of Health and Human Services,
Office of the Inspector General*

20. The Dr. Frea investigation is part of a larger FBI and Department of Health and Human Services, Office of Inspector General (HHS-OIG) investigation into a nationwide telemedicine scheme that has resulted in hundreds of millions of dollars in false and fraudulent claims submitted to Medicare. The scheme involves companies that pay illegal bribes and kickbacks in exchange for signed doctors' prescriptions for DME, such as braces, which the companies submit for payment to Medicare.

21. In this scheme, the doctors who sign the orders for the DME either have no contact with patients or have contact with them through brief telephone calls. In addition, the DME ordered is often medically unnecessary, not eligible for Medicare reimbursement, and/or is not provided as represented.

22. In general, the scheme is operated by telemarketers contacting Medicare beneficiaries and collecting information. The information is then transmitted to a telemedicine doctor for a "consult." The telemedicine consult (which may or may not include a physician speaking with a beneficiary) results in a signed physician order forwarded to a DME supplier which, in turn, bills Medicare for the DME ordered by the telemedicine physician.

23. Based on the nation-wide investigation to date, the first step of the process - patient information collection - is handled by a marketing company.¹ Usually, a Medicare beneficiary responds to a television or online advertisement placed by a marketing company. However, sometimes Medicare beneficiaries are simply cold-called. Subsequently, the patient talks to someone working in a call center (often outside the United States). During this call, the

¹ There was not one single telemedicine brace scheme. There were many overlapping and parallel telemedicine brace schemes. There were variations in exactly how the scheme was performed, including that the same companies often took on more than one role as part of the process. This section of the affidavit is intended to provide the general parameters of a typical brace telemedicine scheme to provide context for Dr. Frea's actions and role in the scheme.

call center representative asks the patient if he/she wants free or low-cost braces, or other DME. The representative confirms that the patient is enrolled with Medicare and collects the patient's Medicare number and other identifying information such as address and phone. The representative then pressures the patient to agree to speak to one of its doctors, rather than the patient's own doctor, claiming that choice would allow the patient to more quickly receive the braces. If the patient agrees to speak to one of the company's doctors, the call center representative forwards the call to a doctor identified by the company to be licensed in the patient's state.

24. The call with the doctor is the next step in the scheme. The doctors typically have a brief, perfunctory consultation with the patient. These consultations sometimes lasted less than a minute, others lasted a few minutes. Some of the "consultations" only involved the doctor reading out the types of braces to be ordered. On other occasions, no telephone conversation took place at all. At the conclusion of the call (when it happens), the doctor authorizes use of his or her electronic signature in a prescription for a brace (or, often, multiple braces such as a back, two knee, two ankle, shoulder, and two elbow braces). The telemedicine companies paid the doctors a fee for each patient, usually \$20 or \$30.

25. The final step in the scheme involves the telemedicine company selling the signed doctors' prescriptions. The telemedicine companies often sold the signed prescriptions to a marketing company, which in turn, resold the signed prescriptions to a DME company that billed Medicare for the braces and ordered and shipped the DME to the patient. In other instances, the telemedicine companies sold signed prescriptions directly to the DME companies.²

² As part of the scheme, as described further herein, the DME companies that billed Medicare paid approximately \$89 per patient order, which could include more than one brace.

26. The scheme has operated in the same or similar manner with other Medicare reimbursable services, including the ordering of, and billing for, expensive cancer genomic (CGx) and pharmacogenetic (PGx) laboratory tests that are medically unnecessary.

III. *Frea's conduct*

27. Dr. Anne Frea is a medical doctor licensed by the State of Wisconsin and has been enrolled as a Medicare provider since 2010. Since 2015, Dr. Frea's practice location on record with Medicare is in Waukesha, Wisconsin.

28. Dr. Frea was identified as an investigative target because her DME prescribing volume appeared to be an outlier compared to other doctors, and because Dr. Frea had been the ordering physician for DME claims by suppliers throughout the country that were already under investigation for the type of health care fraud described above.

29. HHS-OIG analyzed Medicare claims data from January 2015 through April 2020 and found Dr. Frea had no prior relationship with approximately 94% of beneficiaries for whom Dr. Frea prescribed DME, specifically orthotics such as braces for the back, knee, ankle, and shoulder. Not having a prior relationship with a beneficiary patient, or not having provided any billed Medicare services to a beneficiary, can be an indicator of improper or fraudulent services.

30. Additionally, over 70% of the beneficiaries to whom Dr. Frea prescribed knee braces lived outside Wisconsin, including beneficiaries in Illinois, Alabama, and Arizona. This metric indicates that any clinical review for medical necessity and/or exam of the beneficiaries' condition likely took place (if at all) via telemedicine, which is inconsistent with the requirement of an examination for joint laxity for braces billed under Codes L1833 and L1851.

31. The HHS-OIG data analysis further indicated Medicare was billed over \$4,035,000.00 for orthotics ordered by Dr. Frea between January 2015 and April 2020 when Dr.

Frea had no prior relationship with the beneficiary, resulting in Medicare payments of over \$2,125,000.00. Additional HHS-OIG data reports indicate the vast majority of Dr. Frea's DME orders paid by Medicare occurred in three calendar year quarters (nine months) from the third quarter of 2018 through the first quarter of 2019.

32. In March of 2021, investigators conducted several interviews of Medicare beneficiaries. Each of these beneficiaries had received at least one medical brace, which had been ordered by Dr. Frea. Each of the beneficiaries indicated that they had no recollection of speaking with Dr. Frea or being examined by Dr. Frea. The beneficiaries indicated they did not want or need the braces they had received. Many of the beneficiaries had disposed of the braces without ever wearing them. Others still had the braces, unused, in the original packaging.

IV. *Frea's use of email account annefrea22@gmail.com, hosted by Google, LLC*

33. My investigation has demonstrated that evidence of the criminal activity described above is contained in the email accounts anne@frea.us and annefrea22@gmail.com, which are controlled by Dr. Frea.

34. On January 25, 2021, a preservation letter was sent to GoDaddy.com LLC for the account frea.us. On January 26, 2021, a subpoena for records was served to GoDaddy.com LLC. In general, an email that is sent to a GoDaddy.com subscriber is stored in the subscriber's "mailbox" on GoDaddy.com servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on GoDaddy.com servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on GoDaddy.com's servers for a certain period of time.

35. On March 30, 2021, GoDaddy.com responded to a subpoena for subscriber information for anne@frea.us. That response confirmed that anne@frea.us is an active email

account that has been in use from February 18, 2014 to present. A review of the website frea.us, indicates that it is a domain used by a family with the surname “Frea,” and that Dr. Anne Frea is a member of that family.

36. On April 8, 2021, this Court issued a search warrant authorizing investigators to seize copies of emails stored in the anne@frea.us account. On April 9, 2021, officers executed that warrant, and obtained emails responsive to that warrant.

37. In July 2018, Dr. Frea, using her credentials as a medical doctor and attesting as medically necessary, digitally signed a CGx test requisition form of Personalized Genomics, a laboratory operated by an individual under investigation as part of the nationwide telemedicine scheme who has been indicted for health care fraud in another Federal judicial district. Dr. Frea’s digital signature contained the email address anne@frea.us. Medicare data indicates Personalized Genomics first filed a claim for CGx testing ordered by Dr. Frea in June 2018.

38. In January 2019, Dr. Frea entered into an agreement with Luxury Lifestyles Management Inc., a Telemedicine Health Care and Physician Management Organization (Luxury). Luxury was operated by individuals under investigation as part of the nationwide telemedicine scheme and have plead guilty to health care fraud in other Federal judicial districts. A signed copy of the contract between Luxury and Dr. Frea was emailed from anne@frea.us to Pamela Ray (AKA Pamela Edwin), sunrisemedinc.pamela@gmail.com.

39. Email correspondence, using the anne@frea.us account, confirmed that Dr. Frea would be paid at least \$30 per patient consult.

40. Beginning in January of 2019, Dr. Frea received emails sent to anne@frea.us, notifying her of the completion of patient exams.

41. On March 26, 2019, Dr. Frea sent an email from the anne@frea.us to Pamela Edwin at sunrisemedinc.pamela@gmail.com. In the email, Dr. Frea stated she had received a call from United Health Care Medicare regarding a patient's claim that the patient had received medical braces from Dr. Frea. The patient stated they did not know Dr. Frea, and consequently Dr. Frea was being reported for fraud. Dr. Frea informed Edwin that Dr. Frea no longer wanted to work DME cases.

42. A review of the emails contained in the email account anne@frea.us provided to investigators by GoDaddy revealed that Dr. Frea used the additional email address annefrea22@gmail.com to perpetuate the criminal behavior described above.

43. In March of 2018, Dr. Frea received an email from S.S. at Mednick Associates regarding setting up a Mednick Google Calendar. Dr. Frea told S.S. that her email address was annefrea22@gmail.com.

44. In April of 2018, Dr. Frea emailed a copy of her AL license from annefrea22@gmail.com to anne@frea.us.

45. In September of 2018, Dr. Frea digitally signed an independent contractor provider agreement with Bailey Health of Illinois. Notification that the document was ready to be signed and a second notification that the signature had been completed were sent to annefrea22@gmail.com. Notifications of signed service provider agreements were sent to annefrea22@gmail.com for Kansas, Wyoming and Nebraska.

46. Also in September of 2018, Dr. Frea corresponded with M.L. from Simple Health regarding a position as a telemedicine physician. In the email, Dr. Frea discussed the pay rate offered at Simple Health compared to what she was earning though other companies. Simple Health offered to pay physicians \$4 per patient chart review, which M.L. assured Dr Frea, would

yield a minimum of \$100/hour for Dr. Frea. Dr. Frea stated that doing chart reviews for DME, which took 3 – 5 minutes per patient, she earned \$20 - \$30 per patient. During the email chain, Dr. Frea utilized email address anne@frea.us. In the last email of the chain, Dr. Frea stated that M.L. could use the email address annefrea22@gmail.com to set up the review platform utilized by Simple Health.

47. In January of 2019, Dr. Frea responded to an email from Brightside regarding which email account she would like to use. Dr. Frea stated that she would like to use her Gmail account, meaning annefrea22@gmail.com, since this account is the one she uses for “work related items”.

48. On June 3, 2021 a preservation letter was sent for the account annefrea22@gmail.com.

49. Based on my training and experience, it is likely that there are additional emails in the annefrea22@gmail.com account that are relevant to the investigation cannot be obtained through means other than a search of that email account.

BACKGROUND CONCERNING EMAIL

50. In my training and experience, I have learned that Google, LLC provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google, LLC allows subscribers to obtain email accounts at domain names of their creation, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with Google, LLC. During the registration process, Google, LLC asks subscribers to provide basic personal information. Therefore, the computers of Google, LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Google, LLC subscribers) and information concerning subscribers and their use of Google, LLC services, such as account

access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

51. A subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google, LLC. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

52. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

53. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage

of the account. In addition, email providers often have records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

54. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

55. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed

or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

56. Based on the forgoing, I request that the Court issue the proposed search warrant.
57. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google, LLC. Because the warrant will be served on Google, LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with annefrea22@gmail.com, as well as all Google, LLC accounts linked to these accounts by cookie values, creation IP addresses, recovery email, SMS recovery, Android device, telephone numbers, and other similar identifiers, that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) January 25, 2021, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account January 1, 2018 through December 31, 2019, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. Stored web history, cloud-based file storage, social networking profile and friends (connections) list;
- d. Text or voice messages, call logs and associated metadata;
- e. The types of service utilized;

- f. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- g. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.
- h. All records relating to user attribution showing who used or owned the device associated with this account including images, documents, logs, communication records;
- i. Evidence indicating how and when the email account was accessed or used, to determine the chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- j. Evidence indicating the geographic location of email access points at times relevant to the investigation;
- k. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- l. All information that constitutes evidence of violations of 18 U.S.C. § 1347 (health care fraud), 18 U.S.C. § 1035 (false statements relating to health care matters); or contraband or other items illegally possessed; or property designed for use, intended for use, or used in committing violations of 18 U.S.C. § 1347 (health care fraud), 18 U.S.C. § 1035 (false statements relating to health care matters)

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1347 and 18 U.S.C. § 1035, those violations involving **Dr. Anne Frea** and occurring after January 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Records of communications related to: (1) the relationship between Dr. Frea and any Medicare provider, DME supplier, physician staffing company or marketing company dealing with Medicare reimbursable services or items, (2) Dr. Frea's work for, or with, any Medicare provider, DME supplier, physician staffing company or marketing company; (3) the prescription or order of Medicare reimbursable services or items for patients; (4) investigations by Medicare or insurance providers regarding prescribed or ordered health care services or items.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.